(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－5782
（P2001－5782A）
(43)公開日　平成13年１月12日(2001.1.12)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	
12/66		11/20	Ｂ	

審査請求　未請求　請求項の数21　ＯＬ　（全８頁）

(21)出願番号　特願2000－133828(P2000－133828)

(22)出願日　平成12年５月２日(2000.5.2)

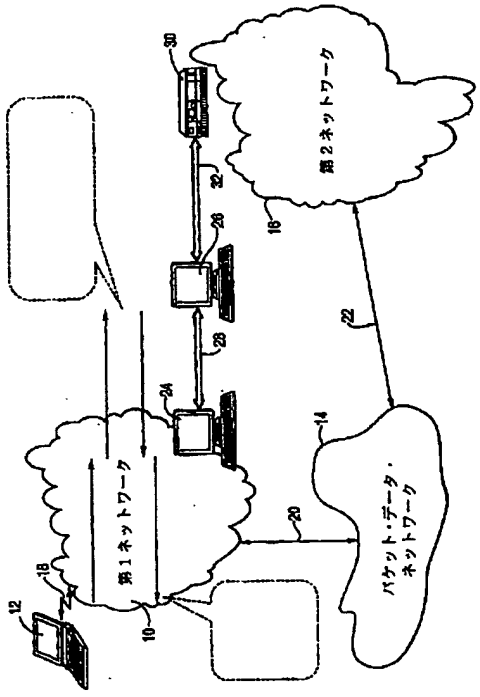
(31)優先権主張番号　０９／３０３４２４
(32)優先日　平成11年５月３日(1999.5.3)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　591275137
ノキア　モービル　フォーンズ　リミテッド
NOKIA MOBILE PHONES LIMITED
フィンランド　02150　エスプー　ケイララーデンティエ　4
(72)発明者　ジュシー　レミライネン
フィンランド　タンペレ　33720　オリヴェデンカツ　16　シー　61
(74)代理人　100086368
弁理士　萩原　誠

最終頁に続く

(54)【発明の名称】　公衆ＩＳＰアクセスネットワークにおける支払方法としてのＳＩＭベースの認証方法と認証システム

(57)【要約】
【課題】　ユーザーのホームネットワークとローミング先ネットワークとの間に課金協定がなくても、ユーザーがローミング先でパケット・データ・ネットワークに接続することを可能とする方法を提供する。
【解決手段】　第２ネットワーク（１６）を通しての該パケット・データ・ネットワーク（１４）との接続をユーザー（１２）に対して承諾するように要求するユーザー要求を第１ネットワーク（１０）に入力し；該ユーザー要求と、該ユーザーによる該パケット・データ・ネットワークの利用についての該第１ネットワークによる該第２ネットワークへの支払いの承認とを該第１ネットワークから該第２ネットワークに送り；該第２ネットワークを通して該パケット・データ・ネットワークとの接続を得ることを該ユーザーに対して承認する認証情報を該第２ネットワークから該第１ネットワークに送り；該パケット・データ・ネットワークとの接続を得るための認証が得られていることを該ユーザーに知らせる該認証情報を該第１ネットワークから該ユーザーに送るステップを含む。



1

【特許請求の範囲】

【請求項１】　パケット・データ・ネットワークとの接続を得る方法であって、この方法は：第２ネットワークを通しての前記パケット・データ・ネットワークとの接続をユーザーに対して承諾するように要求するユーザー要求を第１ネットワークに入力し；前記ユーザー要求と、前記ユーザーによる前記パケット・データ・ネットワークの利用についての前記第１ネットワークによる前記第２ネットワークへの支払いの承認とを前記第１ネットワークから前記第２ネットワークに送り；前記第２ネットワークを通して前記パケット・データ・ネットワークとの接続を得ることを前記ユーザーに対して承認する認証情報を前記第２ネットワークから前記第１ネットワークに送り；前記パケット・データ・ネットワークとの接続を得るための認証が得られていることを前記ユーザーに知らせる前記認証情報を前記第１ネットワークから前記ユーザーに送るステップを含むことを特徴とする方法。

【請求項２】　前記ユーザー要求は前記ユーザーが前記パケット・データ・ネットワークに要求する接続の数量表示を含んでいることを特徴とする請求項１に記載の方法。

【請求項３】　前記数量表示は少なくとも１つのサービス・ユニットを含み、各サービス・ユニットは乱数で符号化されていることを特徴とする請求項２に記載の方法。

【請求項４】　前記各サービス・ユニットは異なる乱数で符号化されることを特徴とする請求項３に記載の方法。

【請求項５】　前記認証情報は、前記ユーザーと前記パケット・データ・ネットワークとの間の機密保護通信メッセージを作るために使用され得る共有されるキーを含むことを特徴とする請求項１に記載の方法。

【請求項６】　前記認証情報は、ｎ個のサービス・ユニットを含む加入者識別モジュールＳＩＭであり、各サービス・ユニットは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答ＳＲＥＳと、前記共有キーＫｃとを含むことを特徴とする請求項５に記載の方法。

【請求項７】　前記認証情報は、前記ユーザーと前記パケット・データ・ネットワークとの間の機密保護通信メッセージを作るために使用され得る共有されるキーを含むことを特徴とする請求項２に記載の方法。

【請求項８】　前記認証情報は、ｎ個のサービス・ユニットを含む加入者識別モジュールＳＩＭであり、各サービス・ユニットは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答ＳＲＥＳと、前記共有キーＫｃとを含むことを特徴とする請求項７に記載の方法。

【請求項９】　前記認証情報は、前記ユーザーと前記パケット・データ・ネットワークとの間の機密保護通信メッセージを作るために使用され得る共有されるキーを含むことを特徴とする請求項３に記載の方法。

2

【請求項１０】　前記第２ネットワークは、サービス・ユニットの数を含む加入者識別モジュールＳＩＭを計算し、各サービス・ユニットは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答と、前記共有キーＫｃとを含むことを特徴とする請求項５に記載の方法。

【請求項１１】　前記認証情報は、前記ユーザーと前記パケット・データ・ネットワークとの間の機密保護通信メッセージを作るために使用され得る共有されるキーを含むことを特徴とする請求項４に記載の方法。

【請求項１２】　前記認証情報は、サービス・ユニットの数を含む加入者識別モジュールＳＩＭであり、各サービスは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答と、前記共有キーとを含むことを特徴とする請求項１１に記載の方法。

【請求項１３】　前記第１ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第２ネットワークへの送信、並びに前記第２ネットワークから前記第１ネットワーク及び前記ユーザーへの前記認証情報の送信とは機密保護通信メッセージによることを特徴とする請求項１に記載の方法。

【請求項１４】　前記第１ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第２ネットワークへの送信、並びに前記第２ネットワークから前記第１ネットワーク及び前記ユーザーへの前記認証情報の送信は機密保護通信メッセージによることを特徴とする請求項２に記載の方法。

【請求項１５】　前記第１ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第２ネットワークへの送信、並びに前記第２ネットワークから前記第１ネットワーク及び前記ユーザーへの前記認証情報の送信は機密保護通信メッセージによることを特徴とする請求項３に記載の方法。

【請求項１６】　前記第１ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第２ネットワークへの送信、並びに前記第２ネットワークから前記第１ネットワーク及び前記ユーザーへの前記認証情報の送信とは機密保護通信メッセージによることを特徴とする請求項４に記載の方法。

【請求項１７】　前記第１ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第２ネットワークへの送信、並びに前記第２ネットワークから前記第１ネットワーク及び前記ユーザーへの前記認証情報の送信とは機密保護通信メッセージによることを特徴とする請求項５に記載の方法。

【請求項１８】　前記パケット・データ・ネットワーク

3

との接続を得るための承認が得られていることがユーザーに知らされた後、前記ユーザーは、乱数ＲＡＮＤと署名入り応答ＳＲＥＳとを含む少なくとも１つのサービス・ユニットについての少なくとも１つの消費要求を前記第２ネットワークに送信し；前記第２ネットワークは、前記ユーザーから受け取った少なくとも１つのサービス・ユニットについての各消費要求の乱数ＲＡＮＤ及び署名入り応答ＳＲＥＳを、蓄積されている乱数ＲＡＮＤ及び署名入り応答ＳＲＥＳと比較して、一致するものがあるか否か判定し；もし一致するものがあれば、前記第２ネットワークは前記ユーザーと前記パケット・データ・ネットワークとの間でデータ・パケットが前記第２ネットワークを通過することを許可することを特徴とする請求項３に記載の方法。

【請求項１９】　前記第２ネットワークは、消費済みサービス・ユニットの数が承諾されたサービス・ユニットの数に等しくなるまで、前記ユーザーに対して承諾されているサービス・ユニットの蓄積されている値から、少なくとも１つのサービス・ユニットについての各消費要求で特定されている消費済みサービス・ユニットの数を借方に記入することを特徴とする請求項１８に記載の方法。

【請求項２０】　未使用の各サービス・ユニットは前記第２ネットワークにおいてハッシュ・テーブルに蓄積され、使用済みの各サービス・ユニットは前記第２ネットワークにおいてハッシュ・テーブルに蓄積されることを特徴とする請求項１９に記載の方法。

【請求項２１】　ユーザーと；前記ユーザーに接続することのできる第１ネットワークと；前記第１ネットワーク及び前記ユーザーに接続することのできる第２ネットワークと；前記第２ネットワークに接続することのできるパケット・データ・ネットワークとを含むシステムにおいて；前記第１ネットワークは、前記ユーザーが前記第２ネットワークを通して前記パケット・データ・ネットワークと接続するための承認を前記第１ネットワークに求めるユーザー要求に応えて、前記ユーザー要求と、前記パケット・データ・ネットワークの前記ユーザーによる利用についての前記第１ネットワークによる支払いの承認とを前記第２ネットワークに送り、前記第２ネットワークは、前記第２ネットワークを通して前記パケット・データ・ネットワークとの接続を得ることを認める認証を前記ユーザーに承諾する認証情報を前記第１ネットワークに送り、前記第１ネットワークは、前記パケット・データ・ネットワークとの接続を得るための認証が得られたことを前記ユーザーに知らせる認証情報を前記ユーザーに送ることを特徴とするシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、パケット・データ・ネットワークへのアクセスの入手についてユーザー

4

（クライアント）に課金する方法及びシステムに関する。

【０００２】

【従来の技術】ユーザー（人、ＰＣ及び電話等の通信装置）は、通常、法人アクセスネットワーク或いは公衆インターネット・サービス・プロバイダ（ＩＳＰ）から提供される接続により、ＩＰネットワーク（インターネット）等のパケット・データ・ネットワークとのアクセスを得る。法人アクセスネットワーク又はＩＳＰから提供される接続は、ユーザーの口座又は会社の口座に料金請求される多数のサービス全部を提供する。それらのサービスは、ユーザーがローミング時にアクセスしたいと望む同じサービスである。場合によっては、例えばユーザーのホーム・ネットワークと、ユーザーがローミングして、それを通してパケット・データ・ネットワークと接続する無線ネットワークとの間にローミング協定が存在するときなど、ユーザーがローミングしているとき、全ての料金はそれぞれのネットワーク間のローミング協定により自動的に処理される。その結果として、第２ネットワークを通してのパケット・データ・ネットワークとのユーザーの接続の結果として生じる課金は、ユーザーと第１ネットワークとの課金契約を通してシームレスに処理される。

【０００３】しかし、パケット・データ・ネットワークへのアクセスをユーザーに提供する無線ネットワークにおいては特にありふれている或る状況においては、或いはユーザーのホーム・ネットワークとユーザーがローミングしてそれを通してパケット・データ・ネットワークに接続するネットワークとの間にユーザーに課金するローミング協定が存在しないとき、典型的ユーザーは第２ネットワークに関して匿名のままでいることを望むことがある。その様な状況では、代わりの課金協定を設けなければならない。

【０００４】ＧＳＭ（Global System for Mobile Communications:移動通信用広域システム）電話システムは、移動ユーザー・ユニットとネットワーク・サーバーとにおいて、ユーザーの認証を制御してネットワークへの無認可のアクセスを防止すると共にユーザー間の通信を暗号化するアルゴリズムを使用する。ＧＳＭシステムは、Mouly及びPautetの刊行物“移動通信のためのＧＳＭシステム（The GSM System for Mobile Communications）”（著作権１９９２）で詳しく解説されている。この刊行物の全体を参照により本書に取り入れる。ＧＳＭネットワークにおける認証は、ユーザーの移動端末装置とネットワークとの両方による署名入り応答ＳＲＥＳの作成により実行され、それはユーザーの移動端末装置に特有の秘密識別子Ｋｉと乱数ＲＡＮＤとの関数である。署名入り応答ＳＲＥＳは、加入者識別モジュール（ＳＩＭ）において、ＳＩＭ内のＫｉと、ネットワーク認証センター（ＡＵＣ）から入手されたＲＡＮＤとに基づいて

5

計算される。また、ユーザーの移動端末装置とネットワークとは、各々、暗号化キーＫｃを作成することにより暗号化を行い、該キーは同じ乱数ＲＡＮＤと該ユーザー移動端末装置の秘密識別子Ｋｉとの関数である。ＳＲＥＳを計算する第１認証アルゴリズムは、Ａ３アルゴリズムとして知られており、ユーザーの移動端末装置が認証される毎に計算されるＫｃを計算する第２アルゴリズムはＡ８アルゴリズムとして知られている。しかし、認証と、暗号化キーＫｃの計算との動作の各々は、前述の計算を実行するように移動端末装置がプログラムされていることを必要とする。

【０００５】

【課題を解決するための手段】本発明は、第２ネットワークを通してのＩＰネットワーク等のパケット・データ・ネットワークとのユーザーの接続についての、ユーザーを代理する第１ネットワークによる第２ネットワークへの支払いの方法及びシステムを提供する。本発明は、ユーザーと、該ユーザーによる第１ネットワークを通しての通信に課金するネットワークのセキュリティ・サーバーと、公衆セキュリティ・サーバーと、ユーザーとパケット・データ・ネットワークとの接続を与える第２ネットワークとの間の一連の通信メッセージを利用する。その一連の通信メッセージはユーザーがユーザー要求を第１ネットワークに入力する購入通信メッセージであり、そのメッセージは、指定された量の通信メッセージのために第２ネットワークを通じてユーザーがパケット・データ・ネットワークと接続できるように認可を要求するものであり、該通信メッセージを以降は“サービス・ユニット”と称する。サービス・ユニットは、無制限に、ユーザーの、第２ネットワークを通じてのパケット・データ・ネットワークとの指定された時間の接続を表わし、或いは、一定額の金銭に対して、サービス・ユニットは接続の時間又はその他の要素に左右される料金構造に応じて変化する量のパケット・データ・ネットワークとの接続時間を提供する。ユーザーのホーム・セキュリティ・サーバーは、第２ネットワークの公衆セキュリティ・サーバーにユーザー要求と、第２ネットワークを通じてのユーザーによるパケット・データ・ネットワークの利用についての第１ネットワークによる第２ネットワークへの支払いの認証とを送る。その後、第２ネットワークは、第２ネットワークを通じてパケット・データ・ネットワークとの接続を得るためのユーザー認証を承諾する認証情報を第１ネットワークに送る。第２ネットワークによる認証情報の計算は、ＧＳＭシステムにおけるＳＩＭと似ている計算を実行する常駐ＳＩＭによって実行される。認証情報は第１ネットワークからユーザーに送られ、情報は、パケット・データ・ネットワークとの接続を得るための認証が得られたことをユーザーに知らせる。ユーザー要求は、パケット・データ・ネットワークとのユーザーの接続の数量表示を含んでおり、その数量表示は少なくとも１つのサービス・ユニットから成り、各々のサービス・ユニットは乱数で符号化されている。好ましくは、各サービス・ユニットは、異なる乱数で符号化される。認証情報は、更に、ユーザーとパケット・データ・ネットワークとの間の機密保護通信メッセージを作るのに使われる共有されるキーを含む。認証情報は、加入者識別モジュールＳＩＭにより計算され、数個（ｎ個）のサービス・ユニットを包含し、各々のサービス・ユニットは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答と、共有キーとを含む。

6

【０００６】好ましくは、第１ネットワークへのユーザー要求の入力、第２ネットワークへのユーザー要求及び支払い認証の送信、並びに第２ネットワークから第１ネットワーク及びユーザーへの認証情報の送信は、秘密通信による。従って、共有される秘密キーＫｃの送信は公開されず、従って、ＧＳＭ通信の場合のようにユーザーとパケット・データ・ネットワークとの後の通信の際にユーザーとパケット・データ・ネットワークとの間に秘密通信を確立するために共有秘密キーＫｃを計算するアルゴリズムをユーザー端末装置が内蔵していなくても良い。

【０００７】パケット・データ・ネットワークへのアクセスが承認され、例えば（それに限らないけれども）ローミング中にパケット・データ・ネットワークへのアクセスが認可され、ユーザーが第２ネットワークへの送信を開始することによってアクセスが開始されたことがユーザーに知らされた後に、承認されたサービス・ユニットの消費が始まり、少なくとも１つのサービス・ユニットの消費についての少なくとも１つの要求は、乱数と署名入り応答とを含む。第２ネットワークは、ユーザーから受け取った少なくとも１つのサービス・ユニットの消費についての各要求の乱数及び署名入り応答を、蓄積されている乱数及び署名入り応答と比較して、一致するか否か確かめる。もし一致するものがあれば、第２ネットワークはデータ・パケットがユーザーとパケット・データ・ネットワークとの間で第２ネットワークを通過することを許す。第２ネットワークは、消費されたサービス・ユニットの数が承諾されたサービス・ユニットの数ｎと等しくなるまで、ユーザーに対して承諾されたサービス・ユニットの蓄積されている値ｎから、少なくとも１つのサービス・ユニットについての各消費要求で特定されている消費済みサービス・ユニットの数を借方に記入する。好ましいアプリケーションでは、未使用の各サービス・ユニットは第２ネットワークにおいて第１リストに蓄積され、各使用済みサービス・ユニットは第２ネットワークにおいて第２リストに蓄積される。好ましくは、その第１及び第２のリストは、サービス・ユニットの、起こる可能性のある衝突を防止するハッシュ・テーブルである。

7

【０００８】本発明のシステムは、ユーザーと；ユーザーと接続できる第１ネットワークと；第１ネットワーク及びユーザーと接続できる第２ネットワークと；第２ネットワークと接続できるパケット・データ・ネットワークとを包含しており；第１ネットワークは、ユーザーが第２ネットワークを通してパケット・データ・ネットワークと接続するための承認を第１ネットワークに求めるユーザー要求に応えて、ユーザー要求と、パケット・データ・ネットワークのユーザーによる利用についての第１ネットワークによる支払いの承認とを第２ネットワークに送り、第２ネットワークは、第２ネットワークを通してパケット・データ・ネットワークとの接続を得ることを認める認証をユーザーに承諾する認証情報を第１ネットワークに送り、第１ネットワークは、パケット・データ・ネッドワークとの接続を得るための認証が得られたことをユーザーに知らせる認証情報をユーザーに送る。

【０００９】全図にわたって、同様の部分を特定するために同様の参照数字及び用語が使われている。

【００１０】

【発明の実施の形態】図１は、第２ネットワーク１６を通してパケット・データ・ネットワーク１４とのユーザー１２（例えばコンピュータ及びモデム）の接続を提供するために第１ネットワーク１０によりユーザー１２に料金請求されるサービス・ユニット購入の図を示している。その購入についての料金請求は、第１ネットワーク１０からユーザー１２に対して行われる。購入されるのは、第２ネットワーク１６経由でのユーザーによるパケット・データ・ネットワーク１４との接続のｎサービス・ユニットであり、それは第２ネットワーク１６を通してのパケット・データ・ネットワークとのユーザーの接続により消費される。第２ネットワークは、単一のエンティティとは限らず、種々の技術で実現され得る複数の地理的に離れているアクセスネットワークから構成されていても良いことが理解されなければならない。第２ネットワークは、ユーザー１２がそれを通してパケット・データ・ネットワーク１４との接続を得る如何なる種類のネットワークであっても良い。図示されているように、第１ネットワークとのユーザー１２の接続は、例えばセルラー、ＰＣＳ、８０２．１１、無線ＬＡＮなど（これらに限定はされない）の任意の種類の無線サービスにより提供される無線リンク１８を経由しているけれども、第１ネットワーク１０との、ワイヤーラインを含むあらゆる種類の接続が本発明の範囲内にあることが理解されなければならない。図示されている通信ライン２０経由でのパケット・データ・ネットワーク１４とのユーザー１２の接続は、在来のものであり、本発明の一部分ではない。購入されたｎサービス・ユニット（ｎは任意の整数である）は、後に図２に示されているように（後述するように）ユーザーが第２ネットワーク１６を

8

通してパケット・データ・ネットワーク１４にアクセスするときに認証とユーザー１２への料金請求とのために使用される。

【００１１】最初の購入シーケンスは、図１に示されているようにｎサービス・ユニットを購入するための４ステップを含んでいる。第１ステップ“１”は、第１ネットワーク１０のホーム・セキュリティ・サーバー２４に送られる、ｎサービス・ユニットの購入を求めるユーザー要求をユーザー１２がユーザーのプロセッサから入力することを含む。ｎサービス・ユニットの購入は、アクセスを提供すると共に、第２ネットワーク１６を通してのパケット・データ・ネットワーク１４との通信の量又は値を指定する。購入されたｎ個のサービス・ユニットは第２ネットワーク１６を通してパケット・データ・ネットワーク１４と接続するための権限をユーザーに与える第１ネットワーク１０のホーム・セキュリティ・サーバー２４に送られ、第２ネットワーク１６は、好ましいアプリケーションでは、ユーザー１２がローミングしているときにパケット・データ・ネットワークとの接続を提供する。

【００１２】第２ステップは、ホーム・セキュリティ・サーバー２４と第２ネットワーク１６の公衆セキュリティ・サーバー２６との間での送信“２”であり、それは各サービス・ユニットに独特の識別乱数ＲＡＮＤを割り当てることによってｎ個のサービス・ユニットを数量表示する。或いは、独特の各ランドは、ユーザー１２によって作られてｎサービス・ユニットの一部分としてホーム・セキュリティ・サーバー２４に回送されても良い。

【００１３】ホーム・セキュリティ・サーバー２４と公衆セキュリティ・サーバー２６との間での通信は、機密保護リンク２８を介して行われる。第２ネットワーク１６のアクセスサーバー３０は、機密保護通信リンク３２により公衆セキュリティ・サーバー２６に接続される。アクセスサーバー３０は、公衆セキュリティ・サーバー２６と共同して、図２との関連で後述するように、機密保護されない通信リンク２２を経由する第２ネットワーク１６とパケット・データ・ネットワーク１４との間でのパケットの通行を制御する。好ましくは、リンク１８経由でのホーム・セキュリティ・サーバー２４へのユーザー要求と、ホーム・セキュリティ・サーバー及び公衆セキュリティ・サーバー２６の間での、第２ネットワーク１６から購入されるべきｎサービス・ユニットを特定するｎ個の乱数の伝送とは機密保護リンクを介して行われる。各々独特の乱数ＲＡＮＤとして個別に符号化されるのが好ましいｎサービス・ユニットの数量表示にくわえて、ホーム・セキュリティ・サーバー２４と公衆セキュリティ・サーバー２６との間での第２伝送“２”は、支払い（電子支払い（Ｅキャッシュ）によるのが好ましい）の授権を含んでいる。しかし、ユーザーのパケット・データ・ネットワーク１４との接続を確保するために

第１ネットワーク１０から第２ネットワーク１６への支払いを清算する任意のメカニズムであって良い。

【００１４】公衆セキュリティ・サーバー２６は、ｎサービス・ユニットを計算して、それを第１リストに蓄積するが、該第１リストは未使用のサービス・ユニットの個数を蓄積するハッシュ・テーブルであるのが好ましい。更に、ハッシュ・テーブルであるのが好ましいかも知れない第２リストは、ｎ個の承認されたサービス・ユニットから消費されたサービス・ユニットを明らかにする。或いは、サービス・ユニットが消費されたら直ちにその消費済みサービス・ユニットを削除することによって第２リストを無くしても良い。ハッシュ・テーブルは、周知のハッシング関数（周知なので、これについては詳しく説明はしない）に依拠するものであり、ｎ個の承認されているサービス・ユニット全部の場所を、その承認から消費に至る過程で、見つけだすための独特のアドレスを提供する。消費段階において、図２に関して後述するように、ユーザー１２のパケット・データ・ネットワーク１４との購入された量（時間又は金額）の接続だけが生じることを保証するために、未使用サービス・ユニットと使用済みサービス・ユニットとが明らかにされる。

【００１５】購入段階の第３ステップは、個々のサービス・ユニットを符号化するのに必要な情報に各々対応するｎ情報トリプレットの形の認証情報の、第２ネットワーク１６の公衆セキュリティ・サーバー２６から第１ネットワークへの送信“３”である。該認証情報は、好ましくは、各サービス・ユニットについて、個々の乱数ＲＡＮＤと、従来技術のＡ３アルゴリズムを用いてＧＳＭ認証により計算される署名入り応答と同様に計算される署名入り応答ＳＲＥＳと、第２ネットワーク１６を通してのユーザー１２とパケット・データ・ネットワーク１４との間での機密保護通信を提供するために使うことのできる暗号化キーＫｃとを含む。暗号化キーＫｃは、図２の消費段階におけるアクセスサーバー３０とユーザー１２との間で共有されるキーでもある。

【００１６】購入段階の第４ステップは送信“４”であり、その間に、ホーム・セキュリティ・サーバー２４は、ＲＡＮＤ、ＳＲＥＳ、Ｋｃのｎトリプレットから成る認証情報を受け取り、データネットワーク１４における消費のためのサービス・ユニットの購入が完了していることをユーザーに知らせるそのｎトリプレットをユーザー１２に回送する。この第４段階で購入シーケンスは完了し、これでユーザー１２は、第２ネットワーク１６を通してのパケット・データ・ネットワーク１４との一定時間単位の接続、又は、時間（ゴールデンアワー及びオフタイム）又はその他の基準の関数として変化する接続を表わす可変数のサービス・ユニットを確保することができる。

【００１７】ユーザー１２が認証情報を受け取るとき、ユーザー及び公衆セキュリティ・サーバー２６は、ｎサービス・ユニットの消費時に第２ネットワーク１６を通じてユーザーとパケット・データ・ネットワーク１４との秘密通信を確立するのに必要な共有暗号化キーＫｃを記憶装置に有することに留意することが重要である。公衆セキュリティ・サーバー２６による署名入り応答ＳＲＥＳ及び共有秘密暗号化キーＫｃの作成並びに秘密通信リンク２８を介して、それをホーム・セキュリティ・サーバー２４に送信し、且つ、ホーム・セキュリティ・サーバーからユーザー１２に送信することは、秘密通信及び／又はユーザー認証を行うのに必要な共有暗号化キーＫｃの初期計算の原因が公衆セキュリティ・サーバー２６であることを考慮すると、ユーザーのプロセッサがサービス・ユニットを購入して消費するのにＡ３及びＡ８アルゴリズム（これらはＧＳＭ認証で利用される）が存在することをサービス・ユニットの購入が必要とするという必要条件を無くする。

【００１８】本発明の方法の第２消費段階は、図２に示されている３つのステップを含んでいる。図示されているように、ユーザー１２は、ローミングし（第１ネットワーク１０との接続から移行している）、リンク１８’（これは無線リンクであるのが好ましいけれども、本発明はそれに限定はされないことが理解されなければならない）を介して第２ネットワーク１６にアクセスする。アクセスサーバー３０は、第２ネットワーク１６へのユーザーのアクセスと、随意に、ｎサービス・ユニットの消費時にユーザー１２とパケット・データ・ネットワーク１４との間でのデータ・パケットの交通とを制御する。しかし、アクセスサーバーはユーザー１２が新たに第２ネットワークと接続するときに認証を行うだけでも良く、その後、アクセスサーバーは、ユーザーが第２ネットワークに接続している間、ユーザーとデータ・パケット１４との間でのデータ交換に全く関わらなくても良い。

【００１９】第１ステップは、パケット・データ・ネットワーク１４との接続についての承認が得られていることがユーザーに知らされた後、ユーザー１２が少なくとも１つのアクセス要求を含む第１通信メッセージ“１”を第２ネットワーク１６のアクセスサーバー３０にリンク１８’を介して送ることを必要とする。各アクセス要求は、各サービス・ユニットの識別情報を構成する個別の乱数ＲＡＮＤ及び署名入り応答ＳＲＥＳを含んでいる。

【００２０】第２ステップは、アクセスサーバー３０から公衆セキュリティ・サーバー２６に中継されるアクセス要求である通信メッセージ“２”を含む。公衆セキュリティ・サーバー２６は、ユーザー１２から受け取った少なくとも１のサービス・ユニットの消費を求める各要求の各乱数ＲＡＮＤ及び署名入り応答ＳＲＥＳを、公衆セキュリティ・サーバーに蓄積されている乱数ＲＡＮＤ

11

及び署名入り応答ＳＲＥＳと比較して一致するものがあるか否か判定する。一致するものが存在することを公衆セキュリティ・サーバー２６が発見すると、第２ネットワーク１６のアクセスサーバー３０は通信メッセージのデータ・パケットがユーザー１２とパケット・データ・ネットワーク１４との間で第２ネットワークを通過することを許す。

【００２１】第２ネットワーク１６の公衆セキュリティ・サーバー２６は、消費済みサービス・ユニットの数が承諾されたサービス・ユニットの数ｎに等しくなるまで、第１ネットワーク１０と第２ネットワーク１６との間で支払条件に達した結果としてユーザー１２に対して承諾された、第１リスト或いはハッシュ・テーブルに蓄積されているサービス・ユニットの値ｎから、少なくとも１つのサービス・ユニットについての各消費要求で特定されている消費済みサービス・ユニットの数を借方に記入する。第２の随意リスト又はハッシュ・テーブルは、公衆セキュリティ・サーバー２６に戻されて消費されたと確認されたサービス・ユニットを蓄積する。従って、承諾されたサービス・ユニットと、消費されたサービス・ユニットと、消費されていないサービス・ユニットとについての合計額が公衆セキュリティ・サーバー２６において常時維持され、或いは、もし第２リストが使われないのであれば、未消費サービス・ユニットの第１リストだけが維持され、消費済みサービス・ユニットはそれから削除される。公衆セキュリティ・サーバー２６が各サービス・ユニットと一致するものを見つけると、各サービス・ユニットの乱数ＲＡＮＤ及び署名入り応答ＳＲＥＳに基づいて該リストから暗号化キーＫｃが計算される。

【００２２】第３ステップは、ユーザー１２とパケット・データ・ネットワーク１４とが第２ネットワーク１６を通して通信することを許可するアクセス承諾である通信メッセージ“３”である。ユーザー１２に対して承諾された、第２ネットワーク１６とパケット・データ・ネットワークとの間の機密保護されない通信路２２を通してのパケット・データ・ネットワーク１４へのアクセス

12

を暗号化するために暗号化キーＫｃが使われる。一方、公衆セキュリティ・サーバー２６に受け取られたサービス・ユニットと、蓄積されているサービス・ユニットとの一致が得られなかったならば、アクセスサーバー３０は、機密保護されない通信路２２を介してのユーザー１２とパケット・データ・ネットワーク１４との接続を拒否する。

【００２３】本発明は、前述したネットワーク・アーキテクチャには限定されなくて、いろいろなネットワーク構成で実施され得るということが理解されなければならない。更に、本発明が実施されるネットワークのデザインは周知されていて、それ自体は本発明の一部分ではない。また、図１及び２の購入及び消費の方法の際にユーザー１２と第１ネットワーク１０と第２ネットワーク１６との間の通信メッセージを符号化するために使われる方法は、本発明の一部分ではないいろいろな方法で達成され得る。

【００２４】本発明をその好ましい実施態様に関して説明したけれども、添付の請求項で定義されている本発明の範囲から逸脱することなく、それに数々の修正を加え得ることが理解されなければならない。その様な修正は全て添付の請求項の範囲に属する。

【図面の簡単な説明】

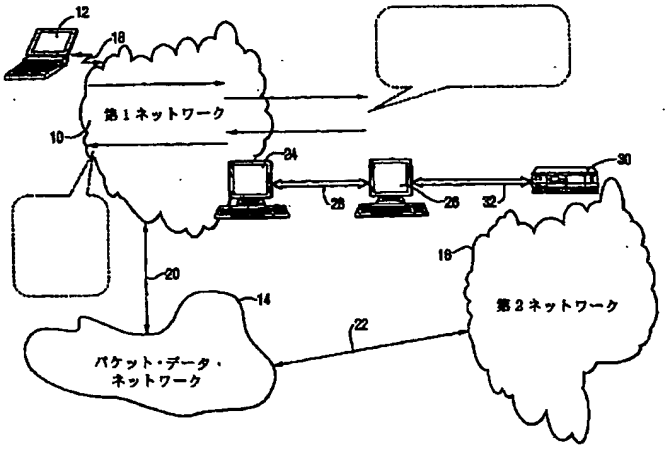
【図１】第２ネットワークを通してパケット・データ・ネットワークとの接続を提供する第１ネットワークでユーザーが本発明に従ってサービス・ユニットを購入する方法を示している。

【図２】第２ネットワークを通してパケット・データ・ネットワークに接続している間に、図１に示されている方法によって得られた購入されたサービス・ユニットのユーザーによる消費を示している。

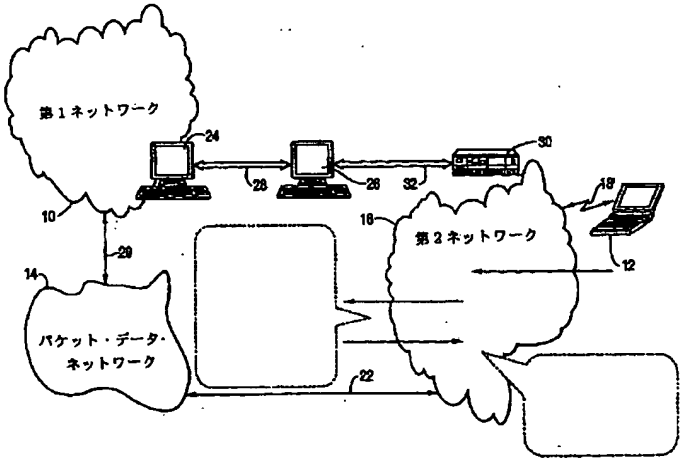
【符号の説明】

１０　第１ネットワーク
１２　ユーザー
１４　パケット・データ・ネットワーク
１６　第２ネットワーク

【図１】



【図２】



フロントページの続き

(72)発明者　ジャンーエリック　エコベルグ
フィンランド　ヘルシンキ　00320　セル
ジャティエ　1　エー　5